PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-298085
(43)Date of publication of application : 12.11.1993

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 04-105034
(22)Date of filing : 24.04.1992

(71)Applicant : FUJITSU LTD
(72)Inventor : AKIYAMA RYOTA
HASEBE TAKAYUKI
YOSHIOKA MAKOTO

(54) SOFTWARE STORAGE MEDIUMSOFTWARE READERAND SOFTWARE MANAGEMENT SYSTEM

(57)Abstract:
PURPOSE: To provide a storage medium which promotes prevention of the wrong use of software circulated to distribution routesa reader for software in this storage mediumand a management system which checks the wrong use of software in the storage medium.
CONSTITUTION: A hybrid storage medium consisting of an un-rewritable storage area 10 and a rewritable storage area 11 is prepared as the storage mediumand password information of software to be presented is recorded in the unrewritable storage area 10and password information consisting of key information for deciphering of ciphered software and the permitted frequency in use of software is recorded in the rewritable storage area 11. Meanwhilethe reader reduces the permitted frequency use of the storage medium in accordance with the use of software to inhibit software from being used more than the permitted frequency in useand the management system checks the wrong use of software in accordance with the display value of the permitted frequency in use of the storage medium.

CLAIMS

[Claim(s)]
[Claim 1]Are software which circulates a distribution channel a software storage medium for recordingand as a software storage mediumA mixed type storage which consists of mixture with a rewriting impossible storage area (10) and a rewritable storage area (11) is preparedWhile taking composition which records coding information of software used as a providing object on a rewriting impossible storage area (10) of this mixed type storageA software storage medium taking

composition which records coding information of key information for decoding code softwareand the number of times of usable of software on a rewritable storage area (11) of this mixed type storage as code protection-of-software information.
[Claim 2]A software storage mediumwherein an initial value of the number of times of usable of software is constituted in the software storage medium according to claim 1 so that it may be recorded in the middle of a distribution channel.
[Claim 3]A software storage medium constituting in the middle of a distribution channel so that this multiplex encryption composition may be changed while taking composition which enciphers code protection-of-software information by a multiple configuration in the software storage medium according to claim 1 or 2.
[Claim 4]A software reader characterized by comprising the following for reading code software recorded on a software storage medium which takes the record composition according to claim 12or 3.
Key information for decoding code software by decoding code protection-of-software information.
The 1st decoding means (40) that decodes the number of times of usable of software.
The 2nd decoding means (41) that decodes code software according to key information which the 1st decoding means (40) of the above decodes.
A calculating means (42) which computes the new number of times of usable by subtracting the number of times of usable which the 1st decoding means (40) of the above decodes for every end of useAn update means (43) which updates the number of times of usable of code protection-of-software information which a software storage medium records according to the new number of times of usable which the above-mentioned calculating means (42) computesA deterrent means (44) controlled so that the 2nd decoding means (41) of the above cannot perform decoding processing when either one of the number of times of usable which the 1st decoding means (40) of the above decodes or the number of times of usable which the above-mentioned calculating means (42) computes displays a zero value.

[Claim 5]The number of times of a use addition which turns into the number of times new when a subtraction value of the number of times of usable reaches a zero value of usable in the software reader according to claim 4 is set upA software reader which carries out the feature of having a setting-out means (45) to update the number of times of usable of code protection-of-software information which a software storage medium records according to this new number of times of usablefollowing a mode which becomes identifiable with the original number of times of usable.
[Claim 6]It is a software management system for managing condition of use of software recorded on a software storage medium which takes the record composition according to claim 12or 3By totaling the number of times of usable of software recorded on a software storage medium collected from a distribution channel. While taking composition which computes a use count of softwarethis use

countA software management system taking composition which compares a summary value of the number of times of usable of software recorded on a software storage medium thrown into a distribution channeland processing so that an unauthorized use of software may be checked according to this comparison result.
[Claim 7]A software management system constituting a total of the number of times of usable of software in the software management system according to claim 6 so that an identification number of a software storage medium may be performed as a unit.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]A software storage medium for this invention to record the software which circulates a distribution channelA software reader for reading the software recorded on the software storage mediumThe software storage medium which can promote prevention of an unauthorized use of the software which circulates a distribution channel especially about the software management system for checking the unauthorized use of the software recorded on the software storage mediumIt is related with the software reader for reading the software recorded on the software storage mediumand the software management system for checking the unauthorized use of the software recorded on the software storage medium.
[0002]These dayscooperating with a communication networkselling the software of a computer programelectronic publishingamusement videoetc. in storessuch as a bookstoreor lending it out in rental storessuch as a video rental shopis performed with development of an information society. the software which circulates such a distribution channel being a distribution leveland it being sold through illegal channels unjustlybeing shopliftedbeing stolen offor being copied unjustly **** -- as -- it will be exposed to an unauthorized use. Such an unauthorized use injures the profits of a software providera storeor a rental store seriously. From now onconstruction of the new mechanism in which prevention of an unauthorized use of the software which circulates a distribution channel is realizable will be cried for.
[0003]
[Description of the Prior Art]When software was sold via the distribution channelby the formerthe method of using IC prepaid card was taken as a method of protecting the software sold.
[0004]Namelythe composition which a medium manufacturing maker enciphers software and records on the nonvolatile storage of CD-ROM etc. which is not rewritable is takenArewhen the software commercial scene is provided with the storage of this code softwareand a userThe composition which purchases the decoding device whose decoding of the code software which this storage is

purchased and also is recorded on a storage is enabledand IC prepaid card in which the number of times of usable which enables starting of this decoding device was recorded is taken. And when are started using IC prepaid card and the number of times of usable of IC prepaid card remainsa decoding device performs decoding of the code software recorded on a storageand takes the composition which subtracts the number of times of usable.

[0005]Since a storage cannot be used without IC prepaid card according to this compositionwhile being able to prevent unjust sale through illegal channels and shoplifter of softwareSince only the number of times of usable which IC prepaid card specifies can use a storagethe illicit copy of software can be prevented now and prevention of an unauthorized use of software can be realized. A user has a recurrence line of the number of times of usable carried outor has you write in the new number of times of usable from a control center via a communication line by mailing the control center of a publishing agency about IC prepaid card in which the number of times of usable is not left behind.

[0006]

[Problem(s) to be Solved by the Invention]Howeverin the sales method of the software according to this conventional technologywhen it sees from the store sidethere is a problem of being hard to perform service for sales promotion which sold software by the piececarried out the salethen was said. When it sees from the user sideeverything but a storage has a problem that IC prepaid card and a decoding device for exclusive use must be managed.

[0007]When it sees from safetysince data tapping from a card connectorand the non-destructive test / duplicate realization in a card chip are possiblethere is a problem that the safety is vulnerableabout IC prepaid card. When it sees from economical efficiencywhile needing expensive IC prepaid cardthere is a problem of needing the expensive decoding device which performs a complicated decoding procedure. When it sees from the control center side of IC prepaid card issue-originthere is a problem that the demand from a user will concentrate.

[0008]Thuswhile the software provider's profits were seriously injured since the unauthorized use of the software which circulates a distribution channel could not be prevented effectively when conventional technology was followedthere was a problem that the profits of a store would be injured seriously.

[0009]This invention was made in view of this situationand is ****. The new software storage medium which can promote prevention of an unauthorized use of the software which circulates the purposeIt is offer with the new software reader for reading the software recorded on the software storage mediumand the new software management system for checking the unauthorized use of the software recorded on the software storage medium.

[0010]

[Means for Solving the Problem]Principle composition of this invention is illustrated to drawing 1. Especially this this invention becomes effective when software which circulates a distribution channel serves as a selling object.

[0011]A software storage medium with which 1 is constituted by this inventiona shipping agency device with which 2 is installed in shipment origin of a maker etc.a relay destination device with which 3 is installed in relay destinationssuch as a rental storea software reader with which 4 is installed in the user sideand 5 are controlling devices installed in a control center etc. Herethis controlling device 5 may be installed in a shipping agency or a relay destination.
[0012]As the software storage medium 1a mixed type storage which consists of mixture with the rewriting impossible storage area 10 and the rewritable storage area 11 is used. The shipping agency device 2 is provided with the following.
The 1st writing means 20 that writes coding information of software of a providing object in the rewriting impossible storage area 10 of the software storage medium 1.
The 2nd writing means 21 that writes code protection-of-software information that protection information of software of a providing object is made in the rewritable storage area 11 of the software storage medium 1.

[0013]Code protection-of-software information written in by this 2nd writing means 21Key information for decoding code software written in by the 1st writing means 20If it consists of coding information with the number of times of usable of software and it is enciphered that key information for decoding code software and the number of times of usable of software are also with the key KY firstNextcomposition enciphered as a multiple configuration is also may be taken as it is enciphered that the coding information is also with the key KST. Hereabout the number of times of usablecomposition written in with the relay destination device 3 may be taken.
[0014]The relay destination device 3 is provided with a code structural change means 30 to change code structure of code protection-of-software information written in by the 2nd writing means 21. If an above-mentioned example explains this code structural change means 30 and code structure of a final stage of code protection-of-software information will be decoded as it is also with the key KSTNextit is performing processing which enciphers the decoded coding information as it is also with the key KX which is different in the key KSTand code structure of code protection-of-software information is changed.
[0015]The software reader 4 is provided with the following.
Key information for decoding code software by decoding code protection-of-software information recorded on the rewritable storage area 11 of the software storage medium 1 given from a relay destination.
The 1st decoding means 40 that decodes the number of times of usable of software.
The 2nd decoding means 41 that decodes code software recorded on the rewriting impossible storage area 10 of the software storage medium 1 according to key information which the 1st decoding means 40 decodes.
The calculating means 42 which computes the new number of times of usable by subtracting the number of times of usable which the 1st decoding means 40

decodes for every end of useThe update means 43 which updates the number of times of usable of code protection-of-software information which the software storage medium 1 records according to the new number of times of usable which the calculating means 42 computesWhen either one of the number of times of usable which the 1st decoding means 40 decodes or the number of times of usable which the calculating means 42 computes displays a zero valueThe deterrent means 44 controlled so that the 2nd decoding means 41 cannot perform decoding processingThe number of times of a use addition used as the number of times new when a subtraction value of the number of times of usable reaches a zero value of usable is set upA setting-out means 45 to update the number of times of usable of code protection-of-software information which the software storage medium 1 records according to this new number of times of usable following a mode which becomes identifiable with the original number of times of usable.

[0016]1st total means 50 by which the controlling device 5 totals the number of times of usable of software recorded on the software storage medium 1 thrown into a distribution channelIt has a comparison means 52 to compare with a summary value of the 2nd total means 51 a summary value of the 2nd total means 51 that totals a use count of softwareand the 1st total means 50 by totaling the number of times of usable of software recorded on the software storage medium 1 collected from a distribution channel. This controlling device 5 may perform an identification number of the software storage medium 1 for a total of the number of times of usable of software as a unit.

[0017]

[Function]As the software storage medium 1 for recording the software which circulates a distribution channel in this inventionWhile taking the composition which records the coding information of the software which prepares the mixed type storage which consists of mixture with the rewriting impossible storage area 10 and the rewritable storage area 11and serves as a providing object in the rewriting impossible storage area 10 of this mixed type storageThe composition which records the coding information of the key information for decoding code software and the number of times of usable of software on the rewritable storage area 11 as code protection-of-software information is taken.

[0018]And the software reader 4 of the users who read the software of this software storage medium 1If the number of times of usable of software is obtained by decoding code protection-of-software informationwhen this number of times of usable will not show the zero valueWhile decoding code software using the key information for code software decoding acquired by decoding code protection-of-software informationThe number of times of usable is subtracted for every end of useand code protection-of-software information is updatedand on the other handwhen this number of times of usable shows the zero valueit processes so that decoding of code software may not be performed.

[0019]Even if software may be sold through illegal channels unjustlymay be shopliftedmay be stolen off or may be exposed to the **********

unauthorized use copied unjustly according to a distribution level by this invention according to this compositionSince use of the software more than the number of times of usable will be eliminated according to the number of times of usable which software and the protection-of-software information recorded in one showworth of the unauthorized use can be reduced greatly. From now onprevention of an unauthorized use of the software which circulates a distribution channel can be aimed at.

[0020]And change the code structure of the software storage medium 1 of a shipping agency to shipare in this compositionprovide the user side with a relay destinationand users' software reader 4If the composition which performs decoding of software by decoding this changed code structure is takensince the unauthorized use between a shipping agency and a relay destination does not make a meaningit can prevent the unauthorized use of software positively.

[0021]In this inventionthe controlling device 5 by the side of a control centerFrom the number of times of usable of the software recorded on the software storage medium 1 collected from the distribution channelwhile computing the summary value of the use count of softwareThe composition which compares this summary value with the summary value of the number of times of usable of the software recorded on the software storage medium 1 thrown into the distribution channel is takenand it processes so that the unauthorized use of software may be checked according to this comparison result.

[0022]Since it can specify which software was used improperly at least for which by the distribution level by this invention according to this compositionthe actual condition of an unauthorized use of software can be grasped correctly. And it is in this compositionand if the composition which performs the identification number of the software storage medium 1 for check processing as a unit is takenthe using-illicit copy etc. specification of whom will be attained by recording the circulation place of the software storage medium 1.

[0023]

[Example]Hereafteraccording to an examplethis invention is explained in detail. An example of the circulation system with which this invention is applied to drawing 2 is illustrated. The circulation system of this figure consists of the maker which ships the software of a subject of protectionthe store which sells the software which a maker shipsa user who purchases the software which a store sellsand a control center which manages the condition of use of software.

[0024]When applying this invention to such a circulation systemthe shipping agency device 2 explained by drawing 1 will be installed in a makerthe relay destination device 3 will be installed in a storethe software reader 4 will be installed in the user sideand the controlling device 5 will be installed in a control center.

[0025]As drawing 1 explainedwhile enciphering the software put on a distribution channel in this invention and recording the coding information on the rewriting impossible storage area 10 of a mixed type storageBy enciphering the protection-of-software information which consists of the key information and the number of

times of usable of software for decoding of the code softwareand taking the composition which records the coding information on the rewritable storage area 11 of the mixed type storage. Prevention of an unauthorized use of software is realized.

[0026]As the this mixture type software storage medium 1while constituting the rewriting impossible storage area 10 from an optical storage mediuma storage which constitutes the rewritable storage area 11 from a magnetic storage medium is usedfor example. It may be made to respond to the ability of the rewriting impossible storage area 10 not to be rewrittenand a ROM area may be called belowand it may be made to respond to the ability of the rewritable storage area 11 to be rewritten although it is nonvolatileand a RAM area may be called below.

[0027]One example of the equipment configuration of the shipping agency device 2 which manages processing by the shipping stage over the mixed type software storage medium 1 which takes this record composition to drawing 3One example of the equipment configuration of the relay destination device 3 which manages processing by the distribution level over this software storage medium 1 in drawing 4One example of the equipment configuration of the controlling device 5 which manages processing in the management stage over this software storage medium 1 in one example of the equipment configuration of the software reader 4 which manages processing in the use stage over this software storage medium 1 in drawing 5and drawing 6 is illustrated.

[0028]Nextaccording to this drawing 3 thru/or drawing 6the mechanism of the protection of software of this invention is explained in detail. The shipping agency device 2 is provided with the 1st encoding means 200the 2nd encoding means 201the 3rd encoding means 202the 1st lock management means 203the 2nd lock management means 204the 3rd lock management means 205and the number-of-times setting-out means 206 of usable as shown in drawing 3.

[0029]When it is when taking this equipment configurationand the software of the plaintext for shipment is given from software enclosurethe 1st encoding means 200By enciphering the software as it is also with the 1st key KU that the 1st lock management means 203 managescode software "E_{KU} (DATA)" is generated and Stamping of the code software is carried out to the ROM area of the mixed type software storage medium 1. HereEOFin the figure by which Stamping is carried out simultaneously displays the end part of the code software.

[0030]Nextthe 1st key KU with which the 2nd encoding means 201 is needed for decoding of code software "E_{KU} (DATA)"Code protection-of-software information "E_{KY} (KUN)" is generated by enciphering the number of times N of usable which the number-of-times setting-out means 206 of usable sets up as it is also with the 2nd key KY that the 2nd lock management means 204 manages. Thenthe 3rd encoding means 202 is enciphering the code protection-of-software information "E_{KY} (KUN)" which the 2nd encoding means 201 outputs as it is also with the 3rd key KST that the 3rd lock management means 205 managesCode protection-of-software information "E_{KST} (E_{KY} (KUN))" is generatedand the code protection-of-software information is electrically written in the RAM area of the mixed type

software storage medium 1.
[0031]And although omitted in this drawing 3the writing means which the shipping agency device 2 does not illustrate will be processed so that the identification number of the software storage medium 1 to ship may be electrically written in the RAM area of that software storage medium 1.
[0032]Thusthe key information for the shipping agency device 2 recording the coding information of the software used as a providing object on the ROM area of the mixed type software storage medium 1and decoding the code software to a RAM area furtherWhile recording the coding information of the protection-of-software information which consists of the number of times of usable of softwareit processes so that the identification number of the software storage medium 1 may be recorded.
[0033]The relay destination device 3 which manages processing by the distribution level over the mixed type software storage medium 1 which takes such record compositionAs shown in drawing 4it has the decoding means 300the 1st encoding means 301the 2nd encoding means 302the 3rd lock management means 303the 4th lock management means 304the conversion lock management means 305and the input means 306.
[0034]When it is when taking this equipment configurationand the software storage medium 1 is received from a makerthe decoding means 300The code protection-of-software information "E_{KST} (E_{KY} (KUN))" currently written in the RAM area of the software storage medium 1By decoding that it is also with the 3rd key KST (the same thing as the key which the 3rd lock management means 205 of the shipping agency device 2 manages) that the 3rd lock management means 303 managescode protection-of-software information "E_{KY} (KUN)" is generated.
[0035]On the other handif the identification number of the software storage medium 1 is inputted from the input means 306the 2nd encoding means 302 will obtain the 4th key KX by enciphering that it is also with the conversion key with which the conversion lock management means 305 manages the identification numberand will register the 4th key KX into the 4th lock management means 304.
[0036]When the decoding means 300 performs decoding processingthenthe 1st encoding means 301The code protection-of-software information "E_{KY} (KUN)" which the decoding means 300 outputs by enciphering that it is also with the 4th key KX that the 4th lock management means 304 manages. Code protection-of-software information "E_{KX} (E_{KY} (KUN))" is generatedand the code protection-of-software information is electrically written in the RAM area of the mixed type software storage medium 1.
[0037]And although omitted in this drawing 4Various kinds of control information like the select code (in this caseit is sale) which indicates whether it is sale and whether the writing means which the relay destination device 3 does not illustrate is a rental will be processed so that it may write in the RAM area of that software storage medium 1 electrically.
[0038]Thusthe code protection-of-software information "E_{KST} (E_{KY} (KUN))" that the relay destination device 3 is written in the RAM area of the software storage

medium 1 supplied from the makerIt processes so that it may rewrite to the thing with another code structure of "E_{KX} (E_{KY} (KUN))."

[0039]The software reader 4 arranged at the user side so that it may mention laterThe composition which decodes the code software "E_{KU} (DATA)" currently written in the ROM area of the software storage medium 1 by taking the composition which decodes code protection-of-software information "E_{KX} (E_{KY} (KUN))" is taken. From now onthe relay destination device 3 the code protection-of-software information currently written in the RAM area of the software storage medium 1 in this wayBy taking the composition rewritten from "E_{KST} (E_{XY} (KUN))" to "E_{KX} (E_{KY} (KUN))." Eliminating thoroughly the unauthorized use of the software storage medium 1 performed between the distribution channels of a store from a maker can be realized.

[0040]The software reader 4 which reads the software of the mixed type software storage medium 1 which takes such record compositionAs shown in drawing 5the 1st encoding means 400 and the 2nd encoding means 401It has the 3rd encoding means 402the 4th encoding means 403the 1st decoding means 404the 2nd decoding means 405the 3rd decoding means 406the status display memory 407the counter 408the comparison means 409the writing means 410and the output means 411.

[0041]When it is when taking this equipment configurationand a user directs reading of the software storage medium 1 purchased from the storefirst the 1st encoding means 400The same key KX as the key which the 4th lock management means 304 of the relay destination device 3 manages is generated by enciphering that it is also with the conversion key to regular about the identification number currently written in the RAM area of the software storage medium 1. Nextthe code protection-of-software information "E_{KX} (E_{KY} (KUN))" that the 1st decoding means 404 is written in the RAM area of the software storage medium 1By decoding that it is also with the key KX which this 1st encoding means 400 generatedcode protection-of-software information "E_{KY} (KUN)" is generated.

[0042]Thenthe 2nd decoding means 405 reads the key KY (the same thing as the key which the 2nd lock management means 204 of the shipping agency device 2 manages) stored in the status display memory 407 by which the battery back-up was carried outBy decoding that it is also with this key KY about the code protection-of-software information "E_{KY} (KUN)" which the 1st decoding means 404 outputs. The key KU which is needed for decoding of the code software "E_{KU} (DATA)" currently recorded on the software storage medium 1and the number of times N of usable of the software (the value and coincidence which the number-of-times setting-out means 206 of usable of the shipping agency device 2 sets up at the beginning of purchase) are generated. And the 2nd decoding means 405 notifies this decoded key KU to the 3rd decoding means 406 while it writes this decoded number of times N of usable in the status display memory 407 and notifies it to the comparison means 409.

[0043]When the notice of the number of times N of usable is received from the 2nd decoding means 405the comparison means 409It confirms whether the number

of times N of usable which received the notice is a zero valuewhen it is a zero valueclear processing of the status display memory 407 is carried outand it processes so that this clear processing may not be performedwhen it is not a zero value. On the other handif the notice of the key KU is received from the 2nd decoding means 405the 3rd decoding means 406The code software "E_{KU} (DATA)" currently written in the ROM area of the software storage medium 1 by decoding that it is also with the key KU which received this notice. The software used as a providing object is generated and the output means 411 is outputted to the output equipment which does not illustrate this decoded software. When the status display memory 407 is cleared at this time as for the 3rd decoding means 406this decoding processing cannot be performed.

[0044]That iswhen the number of times N of usable recorded on the software storage medium 1 is a zero valuethe software reader 4 operates so that use of the software recorded on the software storage medium 1 cannot be performed.

[0045]It is in this processingand if the number of times N of usable developed by the status display memory 407 is read as an initial value of enumerated data and the 3rd decoding means 406 decodes softwarethe counter 408 will be synchronized with this decoding processingand will count down enumerated data. When confirming whether enumerated-data N' reached the zero value in response to the counting processing of this counter 408 at this time and reaching a zero valuethe comparison means 409 clears the status display memory 407in order to forbid use of software.

[0046]And when the end of use of software is detected according to "EOF"the 2nd encoding means 401The new code protection-of-software information "E_{KY} (KUN)" that the number of times of usable was reduced is generated by enciphering that it is also with the key KY about enumerated-data N' of a counterand the key KU. Thenit is enciphering the 3rd encoding means 402 being also with the key KX about the code protection-of-software information "E_{KY} (KUN)" which this 1st encoding means 401 outputsThe new code protection-of-software information "E_{KX} (E_{KY} (KUN))" that the number of times of usable was reduced is generatedand the code protection-of-software information on the RAM area of the software storage medium 1 is rewritten to this new thing.

[0047]When the end of use of software is detected according to "EOF"on the other handthe writing means 410While writing this number of times of usable in the RAM area of the software storage medium 1 as a part of control information by making enumerated-data N' of a counter into the new number of times of usableThe 4th encoding means 403 is written in the RAM area of the software storage medium 1 as a part of control information for the maintenance etc.after enciphering that it is also with the conversion key to regulation of the apparatus-parameters state information read from the status display memory 407.

[0048]Thusthe software reader 4If the number of times of usable of software is obtained by decoding the code protection-of-software information recorded on the software storage medium 1when this number of times of usable will not show the zero valueWhile decoding code software using the key information acquired by

decoding of code protection-of-software information and providing for the userThe number of times of usable is subtracted for every end of useand the code protection-of-software information on the software storage medium 1 is updatedand on the other handwhen this number of times of usable shows the zero valueit processes so that decoding of code software may not be performed.

[0049]Even if software may be sold through illegal channels unjustlymay be shopliftedmay be stolen off or may be exposed to the ********** unauthorized use copied unjustly according to a distribution level by this invention according to this compositionSince use of the software more than the number of times of usable will be eliminated according to the number of times of usable which software and the protection-of-software information recorded in one showworth of the unauthorized use can be greatly reduced nowand prevention of an unauthorized use can be aimed at.

[0050]The controlling device 5 which manages the condition of use of the software of the software storage medium 1 which takes this using formAs shown in drawing 6it has the storage reading means 500the modem means 501the decoding means 502the collation judgment means 503the total comparison means 504the registration medium file 505the store file 506User Information and a soft catalog file 507and the output means 508.

[0051]Arewhen taking this equipment configurationand the decoding means 502If the software storage media 1 are collected via a channel or a store according to the write request etc. of the upgraded softwareBy decoding that it is also with the conversion key to regulation of the code protection-of-software information currently written in the RAM area of the software storage medium 1the number of times of usable currently recorded on the software storage medium 1 is readand it notifies to the total comparison means 504 via the collation judgment means 503.

[0052]On the other handthe collation judgment means 503 is referring to the registration medium file 505when the identification number of the collected software storage medium 1 is received from the storage reading means 500 or the modem means 501By collecting the production information of the software storage medium 1and referring to the store file 506. By pinpointing the store of the software storage medium 1and referring to User Information and the soft catalog file 507. User Information which uses the software storage medium 1and the software information currently recorded on the software storage medium 1 are collectedand the collection and specific result is notified to the total comparison means 504.

[0053]If this collection and specific result is receivedthe total comparison means 504 specifies the identification number of the software storage medium 1 for the number of times of usable in the manufacture time recorded on the software storage medium 1 as a unit according to the production information notified from the collation judgment means 503. And total the identification number of the software storage medium 1 for the number of times of usable notified from the decoding means 502 in a unitand the use count of software is specified from the difference value of the number of times of usable in a manufacture timeand this

summary valueIt confirms whether this specified use count has exceeded the number of times of usable in the manufacture timeand that checked result is outputted to the output means 508.

[0054]Since it can specify which software was used improperly at least for which by the distribution level by this invention according to this compositionthe actual condition of an unauthorized use of software can be grasped correctly. And if it is in this composition and the sale place user name of the software storage medium 1 can be specifiedthe using-illicit copy etc. specification of which user will be attained.

[0055]Although the graphic display example was describedthis invention is not limited to this. For exampleit may be made to record this invention in the store in the middle of circulationalthough the composition which is a shipping agency and records the initial value of the number of times of usable of software was indicated in the examplewithout being restricted to this. It may be made have indicated the composition which does not accept any addition of the number of times of usable in the user sidewhen the number of times of usable in the manufacture time reached the zero valuebut for this invention to accept the addition of the number of times of usable in the examplewithout being restricted to this. Although it is a thing of the usage pattern which sells the software storage medium 1 and being indicated in the examplethis invention may be a thing of the gestalt to lend outwithout being restricted to this.

[0056]

[Effect of the Invention]As explained aboveeven if software may be sold through illegal channels unjustlymay be shopliftedmay be stolen off or may be exposed to the ********** unauthorized use copied unjustly according to a distribution level in this inventionAccording to the number of times of usable which software and the protection-of-software information recorded in one showit used that use of the software more than the number of times of usable would be eliminated.

Therebyworth of the unauthorized use can be greatly reduced now.

From now onprevention of an unauthorized use of the software which circulates a distribution channel can be aimed at. And the unauthorized use between a shipping agency and a relay destination can be thoroughly eliminated by changing code structure in the middle of circulation.

[0057]And in this inventionwhich software can specify now which was used improperly according to a distribution level.

Thereforethe actual condition of an unauthorized use of software can be correctly grasped now.

And if it is possible to record the circulation place of softwarethe using-illicit copy etc. specification of whom will be attained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a principle lineblock diagram of this invention.
[Drawing 2]It is an example of the circulation system with which this invention is applied.
[Drawing 3]It is one example of the equipment configuration of a shipping agency device.
[Drawing 4]It is one example of the equipment configuration of a relay destination device.
[Drawing 5]It is one example of the equipment configuration of a software reader.
[Drawing 6]It is one example of the equipment configuration of a controlling device.
[Description of Notations]
1 Software storage medium
2 Shipping agency device
3 Relay destination device
4 Software reader
5 Controlling device
10 Rewriting impossible storage area
11 A rewritable storage area
20 The 1st writing means
21 The 2nd writing means
30 Code structural change means
40 The 1st decoding means
41 The 2nd decoding means
42 Calculating means
43 Update means
44 Deterrent means
45 Setting-out means
50 The 1st total means
51 The 2nd total means
52 Comparison means

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－298085

(43)公開日　平成５年(1993)11月12日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	４５０　Ｌ	7232－5B		
12/14	３２０　Ｆ	9293－5B		

審査請求　未請求　請求項の数７(全 10 頁)

(21)出願番号　特願平4－105034

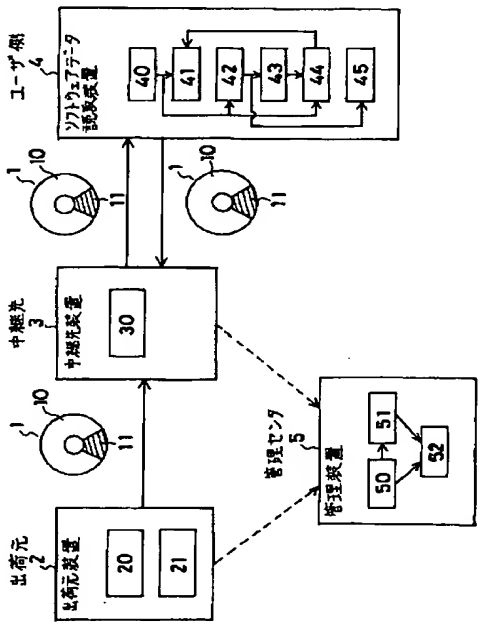
(22)出願日　平成４年(1992)４月24日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　森田　寛　（外１名）

(54)【発明の名称】　ソフトウェア記憶媒体、ソフトウェア読取装置及びソフトウェア管理システム

(57)【要約】
【目的】本発明は、流通経路を流布するソフトウェアの不正使用の防止を促進できる記憶媒体と、その記憶媒体のソフトウェアの読取装置と、その記憶媒体のソフトウェアの不正使用をチェックする管理システムに関する。
【構成】記憶媒体として、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体を用意し、この書換不可能記憶領域１０に、提供対象のソフトウェアの暗号情報を記録するとともに、この書換可能記憶領域１１に、暗号ソフトウェア復号用の鍵情報とソフトウェアの使用可能回数との暗号情報を記録する構成を採り、一方、読取装置は、ソフトウェア使用に応じて記憶媒体の使用可能回数を減じていくとともに、使用可能回数以上のソフトウェア使用を禁止していく構成を取り、一方、管理システムは、記憶媒体の使用可能回数の表示値に従って、ソフトウェアの不正使用をチェックしていくように構成する。

本発明の原理構成図



【特許請求の範囲】
【請求項１】　流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体であって、
ソフトウェア記憶媒体として、書換不可能記憶領域(10)と書換可能記憶領域(11)との混成からなる混成型記憶媒体を用意し、該混成型記憶媒体の書換不可能記憶領域(10)に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、該混成型記憶媒体の書換可能記憶領域(11)に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採ることを、
特徴とするソフトウェア記憶媒体。
【請求項２】　請求項１記載のソフトウェア記憶媒体において、
ソフトウェアの使用可能回数の初期値が、流通経路途中で記録されるよう構成されることを、
特徴とするソフトウェア記憶媒体。
【請求項３】　請求項１又は２記載のソフトウェア記憶媒体において、
暗号ソフトウェア保護情報を多重構成で暗号化していく構成を採るとともに、流通経路途中で、この多重暗号化構成を変更していくよう構成されることを、
特徴とするソフトウェア記憶媒体。
【請求項４】　請求項１、２又は３記載の記録構成を採るソフトウェア記憶媒体に記録される暗号ソフトウェアを読み取るためのソフトウェア読取装置であって、
暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とを復号する第１の復号手段(40)と、
上記第１の復号手段(40)の復号する鍵情報に従って暗号ソフトウェアを復号する第２の復号手段(41)と、
上記第１の復号手段(40)の復号する使用可能回数を使用終了毎に減算することで新たな使用可能回数を算出する算出手段(42)と、
上記算出手段(42)の算出する新たな使用可能回数に従って、ソフトウェア記憶媒体の記録する暗号ソフトウェア保護情報の使用可能回数を更新する更新手段(43)と、
上記第１の復号手段(40)の復号する使用可能回数か、上記算出手段(42)の算出する使用可能回数のいずれか一方がゼロ値を表示するときには、上記第２の復号手段(41)が復号処理を実行できないように制御する抑止手段(44)とを備えることを、
特徴するソフトウェア読取装置。
【請求項５】　請求項４記載のソフトウェア読取装置において、
使用可能回数の減算値がゼロ値に達するときに新たな使用可能回数となる使用追加回数を設定して、本来の使用可能回数と識別可能となる態様に従いつつ、この新たな使用可能回数に従ってソフトウェア記憶媒体の記録する暗号ソフトウェア保護情報の使用可能回数を更新する設定手段(45)を備えることを、
特徴するソフトウェア読取装置。
【請求項６】　請求項１、２又は３記載の記録構成を採るソフトウェア記憶媒体に記録されるソフトウェアの使用状態を管理するためのソフトウェア管理システムであって、
流通経路から回収したソフトウェア記憶媒体に記録されるソフトウェアの使用可能回数を集計していくことで、ソフトウェアの使用回数を算出する構成を採るとともに、この使用回数と、流通経路に投入したソフトウェア記憶媒体に記録されるソフトウェアの使用可能回数の集計値とを比較する構成を採って、この比較結果に従ってソフトウェアの不正使用をチェックしていくよう処理することを、
特徴とするソフトウェア管理システム。
【請求項７】　請求項６記載のソフトウェア管理システムにおいて、
ソフトウェアの使用可能回数の集計を、ソフトウェア記憶媒体の識別番号を単位として実行していくよう構成されることを、
特徴とするソフトウェア管理システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関し、特に、流通経路を流布するソフトウェアの不正使用の防止を促進できるソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関する。
【０００２】最近、情報化社会の発達に伴って、コンピュータプログラムや電子出版や娯楽ビデオ等のソフトウェアを、通信ネットワークと連携して、書店等の販売店で販売したり、レンタルビデオ店等のレンタル店で貸し出していくことが行われている。このような流通経路を流布するソフトウェアは、流通段階で、不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されたりというように不正使用にさらされることになる。このような不正使用は、ソフトウェア提供者や販売店やレンタル店の利益を著しく害する。これから、流通経路を流布するソフトウェアの不正使用の防止を実現できる新たな仕組みの構築が叫ばれているのである。
【０００３】
【従来の技術】流通経路を介してソフトウェアを販売し

ていく場合に、販売されるソフトウェアを保護する方法として、従来では、ＩＣプリペードカードを用いる方法を採っていた。

【０００４】すなわち、媒体製造メーカが、ソフトウェアを暗号化してＣＤ－ＲＯＭ等の書き換え不可能な不揮発性の記憶媒体に記録する構成を採って、この暗号ソフトウェアの記憶媒体をソフトウェア市場に提供していくときにあって、ユーザは、この記憶媒体を購入する他に、記憶媒体に記録される暗号ソフトウェアを復号可能とする復号装置と、この復号装置の起動を可能にする使用可能回数の記録されたＩＣプリペードカードとを購入する構成を採る。そして、復号装置は、ＩＣプリペードカードを使って起動されるときに、ＩＣプリペードカードの使用可能回数が残っている場合には、記憶媒体に記録される暗号ソフトウェアの復号を実行し、その使用可能回数を減算していく構成を採る。

【０００５】この構成に従い、ＩＣプリペードカードがなければ記憶媒体を使用することができないことから、ソフトウェアの不正横流しや万引きを防止できるようになるとともに、ＩＣプリペードカードの指定する使用可能回数しか記憶媒体を使用することができないことから、ソフトウェアの不正複写を防止できるようになり、ソフトウェアの不正使用の防止を実現できることになる。なお、ユーザは、使用可能回数の残されていないＩＣプリペードカードについては、発行元の管理センタに郵送することで使用可能回数を再発行してもらったり、通信回線を介して管理センタから新たな使用可能回数を書き込んでもらったりすることになる。

【０００６】

【発明が解決しようとする課題】しかしながら、この従来技術に従うソフトウェアの販売方法では、販売店の側から見ると、ソフトウェアを切り売りしたり、バーゲンセールしたりするといったような販売促進の為のサービスが実行しにくいという問題点がある。また、ユーザの側から見ると、記憶媒体の他に、ＩＣプリペードカードと専用の復号装置とを管理しなければならないという問題点がある。

【０００７】また、安全性から見ると、ＩＣプリペードカードについては、カードコネクタからのデータ盗聴と、カードチップ内の非破壊検査／複製実現とが可能であることから、その安全性が脆弱であるという問題点がある。また、経済性から見ると、高価なＩＣプリペードカードを必要とするとともに、複雑な復号手順を実行する高価な復号装置を必要とするという問題点がある。また、ＩＣプリペードカードの発行元の管理センタ側から見ると、ユーザからの要求が集中することになるという問題点がある。

【０００８】このように、従来技術に従っていると、流通経路を流布するソフトウェアの不正使用を有効に防止することができないことから、ソフトウェア提供者の利益が著しく害されるとともに、販売店の利益が著しく害されることになるという問題点があった。

【０００９】本発明はかかる事情に鑑みてなされたものであって、流通経路を流布するソフトウェアの不正使用の防止を促進できる新たなソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るための新たなソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするための新たなソフトウェア管理システムとの提供を目的とするものである。

【００１０】

【課題を解決するための手段】図１に本発明の原理構成を図示する。この本発明は、特に、流通経路を流布するソフトウェアが販売対象となるときに有効となるものである。

【００１１】１は本発明により構成されるソフトウェア記憶媒体、２はメーカ等の出荷元に設置される出荷元装置、３はレンタル店等の中継先に設置される中継先装置、４はユーザ側に設置されるソフトウェア読取装置、５は管理センタ等に設置される管理装置である。ここで、この管理装置５は、出荷元や中継先に設置されることもある。

【００１２】ソフトウェア記憶媒体１としては、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体が用いられる。出荷元装置２は、ソフトウェア記憶媒体１の書換不可能記憶領域１０に、提供対象のソフトウェアの暗号情報を書き込む第１の書込手段２０と、ソフトウェア記憶媒体１の書換可能記憶領域１１に、提供対象のソフトウェアの保護情報をなす暗号ソフトウェア保護情報を書き込む第２の書込手段２１とを備える。

【００１３】この第２の書込手段２１により書き込まれる暗号ソフトウェア保護情報は、第１の書込手段２０により書き込まれる暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数との暗号情報からなり、先ず最初に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数とが鍵ＫＹでもって暗号化されると、次に、その暗号情報が鍵ＫＳＴでもって暗号化されるというように、多重構成でもって暗号化されていく構成を採ることがある。ここで、使用可能回数については、中継先装置３で書き込まれる構成が採られることもある。

【００１４】中継先装置３は、第２の書込手段２１により書き込まれる暗号ソフトウェア保護情報の暗号構造を変更する暗号構造変更手段３０を備える。この暗号構造変更手段３０は、上述の例で説明するならば、鍵ＫＳＴでもって暗号ソフトウェア保護情報の最終段の暗号構造を復号すると、次に、その復号された暗号情報を鍵ＫＳＴとは異なる鍵ＫＸでもって暗号化するような処理を実行していくことで、暗号ソフトウェア保護情報の暗号構

造を変更する。

【００１５】ソフトウェア読取装置４は、中継先から与えられるソフトウェア記憶媒体１の書換可能記憶領域１１に記録される暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とを復号する第１の復号手段４０と、第１の復号手段４０の復号する鍵情報に従って、ソフトウェア記憶媒体１の書換不可能記憶領域１０に記録される暗号ソフトウェアを復号する第２の復号手段４１と、第１の復号手段４０の復号する使用可能回数を使用終了毎に減算することで新たな使用可能回数を算出する算出手段４２と、算出手段４２の算出する新たな使用可能回数に従って、ソフトウェア記憶媒体１の記録する暗号ソフトウェア保護情報の使用可能回数を更新する更新手段４３と、第１の復号手段４０の復号する使用可能回数か、算出手段４２の算出する使用可能回数のいずれか一方がゼロ値を表示するときには、第２の復号手段４１が復号処理を実行できないように制御する抑止手段４４と、使用可能回数の減算値がゼロ値に達するときに新たな使用可能回数となる使用追加回数を設定して、本来の使用可能回数と識別可能となる態様に従いつつ、この新たな使用可能回数に従ってソフトウェア記憶媒体１の記録する暗号ソフトウェア保護情報の使用可能回数を更新する設定手段４５とを備える。

【００１６】管理装置５は、流通経路に投入されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数を集計する第１の集計手段５０と、流通経路から回収されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数を集計していくことで、ソフトウェアの使用回数を集計する第２の集計手段５１と、第１の集計手段５０の集計値と第２の集計手段５１の集計値とを比較する比較手段５２とを備える。この管理装置５は、ソフトウェアの使用可能回数の集計をソフトウェア記憶媒体１の識別番号を単位として実行していくことがある。

【００１７】

【作用】本発明では、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体１として、書換不可能記憶領域１０と書換可能記憶領域１１との混成からなる混成型記憶媒体を用意し、この混成型記憶媒体の書換不可能記憶領域１０に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、書換可能記憶領域１１に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能回数との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採る。

【００１８】そして、このソフトウェア記憶媒体１のソフトウェアを読み取るユーザ側のソフトウェア読取装置４は、暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能回数を得ると、この使用可能回数がゼロ値を表示していないときには、暗号ソフトウェア保護情報を復号することで得られる暗号ソフトウェア復号用の鍵情報を用いて暗号ソフトウェアを復号するとともに、使用終了毎に使用可能回数を減算して暗号ソフトウェア保護情報を更新し、一方、この使用可能回数がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理する。

【００１９】この構成に従い、本発明では、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになるのである。

【００２０】そして、この構成にあって、中継先は、出荷元の出荷するソフトウェア記憶媒体１の暗号構造を変更してユーザ側に提供し、ユーザ側のソフトウェア読取装置４は、この変更された暗号構造を復号することでソフトウェアの復号を実行していく構成を採ると、出荷元と中継先との間での不正使用は意味をなさないことから、ソフトウェアの不正使用を積極的に防止することができるようになる。

【００２１】更に、本発明では、管理センタ側の管理装置５は、流通経路から回収されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数から、ソフトウェアの使用回数の集計値を算出するとともに、この集計値と、流通経路に投入されたソフトウェア記憶媒体１に記録されるソフトウェアの使用可能回数の集計値とを比較する構成を採って、この比較結果に従ってソフトウェアの不正使用をチェックしていくよう処理する。

【００２２】この構成に従い、本発明では、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。そして、この構成にあって、チェック処理をソフトウェア記憶媒体１の識別番号を単位として実行していく構成を採ると、ソフトウェア記憶媒体１の流通先を記録しておくことで、誰が不正複写等の不正使用をしたのかも特定可能となるのである。

【００２３】

【実施例】以下、実施例に従って本発明を詳細に説明する。図２に、本発明の適用される流通システムの一例を図示する。この図の流通システムは、保護対象のソフトウェアを出荷するメーカと、メーカの出荷するソフトウェアを販売する販売店と、販売店の販売するソフトウェアを購入するユーザと、ソフトウェアの使用状態を管理する管理センタとからなる。

【００２４】このような流通システムに本発明を適用す

る場合、図１で説明した出荷元装置２はメーカに設置され、中継先装置３は販売店に設置され、ソフトウェア読取装置４はユーザ側に設置され、管理装置５は管理センタに設置されることになる。

【００２５】図１で説明したように、本発明では、流通経路に置かれるソフトウェアを暗号化して、その暗号情報を混成型記憶媒体の書換不可能記憶領域１０に記録するとともに、その暗号ソフトウェアの復号のための鍵情報と、そのソフトウェアの使用可能回数とからなるソフトウェア保護情報を暗号化して、その暗号情報をその混成型記憶媒体の書換可能記憶領域１１に記録する構成を採ることで、ソフトウェアの不正使用の防止を実現するものである。

【００２６】この混成型のソフトウェア記憶媒体１としては、例えば、書換不可能記憶領域１０を光記憶媒体で構成するとともに、書換可能記憶領域１１を磁気記憶媒体で構成するような記憶媒体が用いられる。なお、書換不可能記憶領域１０を書き換えが不可能であることに対応させて、以下ＲＯＭ領域と称することがあり、また、書換可能記憶領域１１を不揮発性ではあるが、書き換えが可能であることに対応させて、以下ＲＡＭ領域と称することがある。

【００２７】図３に、この記録構成を採る混成型のソフトウェア記憶媒体１に対しての出荷段階での処理を司る出荷元装置２の装置構成の一実施例、図４に、このソフトウェア記憶媒体１に対しての流通段階での処理を司る中継先装置３の装置構成の一実施例、図５に、このソフトウェア記憶媒体１に対しての使用段階での処理を司るソフトウェア読取装置４の装置構成の一実施例、図６に、このソフトウェア記憶媒体１に対しての管理段階での処理を司る管理装置５の装置構成の一実施例を図示する。

【００２８】次に、この図３ないし図６に従って、本発明のソフトウェア保護のメカニズムについて詳細に説明する。出荷元装置２は、図３に示すように、第１の暗号化手段２００と、第２の暗号化手段２０１と、第３の暗号化手段２０２と、第１の鍵管理手段２０３と、第２の鍵管理手段２０４と、第３の鍵管理手段２０５と、使用可能回数設定手段２０６とを備える。

【００２９】この装置構成を採るときにあって、ソフトウェア格納装置から出荷対象の平文のソフトウェアが与えられると、第１の暗号化手段２００は、そのソフトウェアを第１の鍵管理手段２０３の管理する第１の鍵ＫＵでもって暗号化することで、暗号ソフトウェア“E_{KU}（ＤＡＴＡ）”を生成して、その暗号ソフトウェアを混成型のソフトウェア記憶媒体１のＲＯＭ領域にスタンピングする。ここで、同時にスタンピングされる図中の“ＥＯＦ”は、その暗号ソフトウェアの終了箇所を表示するものである。

【００３０】次に、第２の暗号化手段２０１は、暗号ソフトウェア“E_{KU}（ＤＡＴＡ）”の復号に必要となる第１の鍵ＫＵと、使用可能回数設定手段２０６の設定する使用可能回数Ｎとを、第２の鍵管理手段２０４の管理する第２の鍵ＫＹでもって暗号化することで、暗号ソフトウェア保護情報“E_{KY}（ＫＵ，Ｎ）”を生成する。続いて、第３の暗号化手段２０２は、第２の暗号化手段２０１の出力する暗号ソフトウェア保護情報“E_{KY}（ＫＵ，Ｎ）”を、第３の鍵管理手段２０５の管理する第３の鍵ＫＳＴでもって暗号化することで、暗号ソフトウェア保護情報“E_{KST}（E_{KY}（ＫＵ，Ｎ））”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込む。

【００３１】そして、この図３では省略してあるが、出荷元装置２の図示しない書込手段は、出荷するソフトウェア記憶媒体１の識別番号をそのソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込んでいくよう処理することになる。

【００３２】このようにして、出荷元装置２は、混成型のソフトウェア記憶媒体１のＲＯＭ領域に、提供対象となるソフトウェアの暗号情報を記録し、更に、ＲＡＭ領域に、その暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能回数とからなるソフトウェア保護情報の暗号情報を記録するとともに、ソフトウェア記憶媒体１の識別番号を記録していくよう処理するのである。

【００３３】このような記録構成を採る混成型のソフトウェア記憶媒体１に対しての流通段階での処理を司る中継先装置３は、図４に示すように、復号手段３００と、第１の暗号化手段３０１と、第２の暗号化手段３０２と、第３の鍵管理手段３０３と、第４の鍵管理手段３０４と、変換鍵管理手段３０５と、入力手段３０６とを備える。

【００３４】この装置構成を採るときにあって、メーカからソフトウェア記憶媒体１を受け取ると、復号手段３００は、そのソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報“E_{KST}（E_{KY}（ＫＵ，Ｎ））”を、第３の鍵管理手段３０３の管理する第３の鍵ＫＳＴ（出荷元装置２の第３の鍵管理手段２０５の管理する鍵と同一のもの）でもって復号することで、暗号ソフトウェア保護情報“E_{KY}（ＫＵ，Ｎ）”を生成する。

【００３５】一方、第２の暗号化手段３０２は、入力手段３０６からソフトウェア記憶媒体１の識別番号が入力されてくると、その識別番号を変換鍵管理手段３０５の管理する変換鍵でもって暗号化することで第４の鍵ＫＸを得て、その第４の鍵ＫＸを第４の鍵管理手段３０４に登録する。

【００３６】復号手段３００が復号処理を実行すると、続いて、第１の暗号化手段３０１は、復号手段３００の出力する暗号ソフトウェア保護情報“E_{KY}（ＫＵ，

Ｎ）″を、第４の鍵管理手段３０４の管理する第４の鍵ＫＸでもって暗号化することで、暗号ソフトウェア保護情報″E_{KX}（E_{KY}（ＫＵ，Ｎ））″を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込む。

【００３７】そして、この図４では省略してあるが、中継先装置３の図示しない書込手段は、販売なのかレンタルなのかを表示する選択コード（この場合は販売である）のような各種の制御情報を、そのソフトウェア記憶媒体１のＲＡＭ領域に電気的に書き込んでいくよう処理することになる。

【００３８】このようにして、中継先装置３は、メーカから供給されたソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報″E_{KST}（E_{KY}（ＫＵ，Ｎ））″を、″E_{KX}（E_{KY}（ＫＵ，Ｎ））″という別の暗号構造を持つものに書き換えていくよう処理するのである。

【００３９】後述するように、ユーザ側に配置されるソフトウェア読取装置４は、暗号ソフトウェア保護情報″E_{KX}（E_{KY}（ＫＵ，Ｎ））″を復号する構成を採ることで、ソフトウェア記憶媒体１のＲＯＭ領域に書き込まれている暗号ソフトウェア″E_{KU}（ＤＡＴＡ）″を復号していく構成を採るものである。これから、このように、中継先装置３が、ソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報を、″E_{KST}（E_{XY}（ＫＵ，Ｎ））″から″E_{KX}（E_{KY}（ＫＵ，Ｎ））″に書き換えていく構成を採ることで、メーカから販売店の流通経路の間で行われるソフトウェア記憶媒体１の不正使用を完全に排除することが実現できることになる。

【００４０】このような記録構成を採る混成型のソフトウェア記憶媒体１のソフトウェアを読み取るソフトウェア読取装置４は、図５に示すように、第１の暗号化手段４００と、第２の暗号化手段４０１と、第３の暗号化手段４０２と、第４の暗号化手段４０３と、第１の復号手段４０４と、第２の復号手段４０５と、第３の復号手段４０６と、状態表示メモリ４０７と、カウンタ４０８と、比較手段４０９と、書込手段４１０と、出力手段４１１とを備える。

【００４１】この装置構成を採るときにあって、ユーザが販売店から購入したソフトウェア記憶媒体１の読み取りを指示すると、先ず最初に、第１の暗号化手段４００は、そのソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている識別番号を、規定の変換鍵でもって暗号化することで、中継先装置３の第４の鍵管理手段３０４の管理する鍵と同一の鍵ＫＸを生成する。次に、第１の復号手段４０４は、ソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報″E_{KX}（E_{KY}（ＫＵ，Ｎ））″を、この第１の暗号化手段４００の生成した鍵ＫＸでもって復号することで、暗号ソフトウェア保護情報″E_{KY}（ＫＵ，Ｎ）″を生成する。

【００４２】続いて、第２の復号手段４０５は、バッテリバックアップされた状態表示メモリ４０７に格納されている鍵ＫＹ（出荷元装置２の第２の鍵管理手段２０４の管理する鍵と同一のもの）を読み出し、第１の復号手段４０４の出力する暗号ソフトウェア保護情報″E_{KY}（ＫＵ，Ｎ）″を、この鍵ＫＹでもって復号することで、ソフトウェア記憶媒体１に記録されている暗号ソフトウェア″E_{KU}（ＤＡＴＡ）″の復号に必要となる鍵ＫＵと、そのソフトウェアの使用可能回数Ｎ（購入当初は、出荷元装置２の使用可能回数設定手段２０６の設定する値と一致）とを生成する。そして、第２の復号手段４０５は、この復号した使用可能回数Ｎを状態表示メモリ４０７に書き込み、比較手段４０９に通知していくとともに、この復号した鍵ＫＵを第３の復号手段４０６に通知していく。

【００４３】第２の復号手段４０５から使用可能回数Ｎの通知を受け取ると、比較手段４０９は、通知を受けた使用可能回数Ｎがゼロ値であるか否かをチェックして、ゼロ値であるときには状態表示メモリ４０７をクリア処理し、ゼロ値でないときにはこのクリア処理を実行しないよう処理する。一方、第３の復号手段４０６は、第２の復号手段４０５から鍵ＫＵの通知を受け取ると、ソフトウェア記憶媒体１のＲＯＭ領域に書き込まれている暗号ソフトウェア″E_{KU}（ＤＡＴＡ）″を、この通知を受けた鍵ＫＵでもって復号することで、提供対象となるソフトウェアを生成し、出力手段４１１は、この復号されたソフトウェアを図示しない出力機器に出力していく。このとき、第３の復号手段４０６は、状態表示メモリ４０７がクリアされているときには、この復号処理を実行できない。

【００４４】すなわち、ソフトウェア記憶媒体１に記録される使用可能回数Ｎがゼロ値であるときには、ソフトウェア読取装置４は、ソフトウェア記憶媒体１に記録されたソフトウェアの使用を実行できないように動作していくのである。

【００４５】この処理にあって、カウンタ４０８は、状態表示メモリ４０７に展開された使用可能回数Ｎを計数値の初期値として読み込んで、第３の復号手段４０６がソフトウェアの復号を行うと、この復号処理に同期させて計数値をカウントダウンする。このとき、比較手段４０９は、このカウンタ４０８の計数処理を受けて、計数値Ｎ′がゼロ値に達したか否かをチェックして、ゼロ値に達するときには、ソフトウェアの使用を禁止するために状態表示メモリ４０７をクリアしていく。

【００４６】そして、″ＥＯＦ″に従ってソフトウェアの使用の終了が検出されると、第２の暗号化手段４０１は、カウンタの計数値Ｎ′と鍵ＫＵとを、鍵ＫＹでもって暗号化することで、使用可能回数の減じられた新たな暗号ソフトウェア保護情報″E_{KY}（ＫＵ，Ｎ）″を生成

する。続いて、第３の暗号化手段４０２は、この第１の暗号化手段４０１の出力する暗号ソフトウェア保護情報“E_{KY}（ＫＵ，Ｎ）”を、鍵ＫＸでもって暗号化することで、使用可能回数の減じられた新たな暗号ソフトウェア保護情報“E_{KX}（E_{KY}（ＫＵ，Ｎ））”を生成して、ソフトウェア記憶媒体１のＲＡＭ領域の暗号ソフトウェア保護情報をこの新たなものに書き換えていく。

【００４７】一方、“ＥＯＦ”に従ってソフトウェアの使用の終了が検出されると、書込手段４１０は、カウンタの計数値Ｎ′を新たな使用可能回数として、この使用可能回数を制御情報の一部としてソフトウェア記憶媒体１のＲＡＭ領域に書き込んでいくとともに、第４の暗号化手段４０３は、状態表示メモリ４０７から読み出す装置パラメータ状態情報を規定の変換鍵でもって暗号化してから、制御情報の一部としてソフトウェア記憶媒体１のＲＡＭ領域にメンテナンス等のために書き込んでいく。

【００４８】このようにして、ソフトウェア読取装置４は、ソフトウェア記憶媒体１に記録される暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能回数を得ると、この使用可能回数がゼロ値を表示していないときには、暗号ソフトウェア保護情報の復号により得られる鍵情報を用いて暗号ソフトウェアを復号してユーザに提供していくとともに、使用終了毎に使用可能回数を減算してソフトウェア記憶媒体１の暗号ソフトウェア保護情報を更新し、一方、この使用可能回数がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理するのである。

【００４９】この構成に従い、本発明では、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになって、不正使用の防止を図れることになる。

【００５０】この使用形態を採るソフトウェア記憶媒体１のソフトウェアの使用状態を管理する管理装置５は、図６に示すように、記憶媒体読取手段５００と、モデム手段５０１と、復号手段５０２と、照合分別手段５０３と、集計比較手段５０４と、登録媒体ファイル５０５と、販売店ファイル５０６と、ユーザ情報・ソフトカタログファイル５０７と、出力手段５０８とを備える。

【００５１】この装置構成を採るときにあって、復号手段５０２は、バージョンアップしたソフトウェアの書込要求等に従って通信路や販売店を介してソフトウェア記憶媒体１が回収されると、そのソフトウェア記憶媒体１のＲＡＭ領域に書き込まれている暗号ソフトウェア保護情報を規定の変換鍵でもって復号することで、そのソフトウェア記憶媒体１に記録されている使用可能回数を読み取って、照合分別手段５０３を介して集計比較手段５０４に通知する。

【００５２】一方、照合分別手段５０３は、記憶媒体読取手段５００やモデム手段５０１から、回収されたソフトウェア記憶媒体１の識別番号を受け取ると、登録媒体ファイル５０５を参照することで、そのソフトウェア記憶媒体１の製造情報を収集し、販売店ファイル５０６を参照することで、そのソフトウェア記憶媒体１の販売店を特定し、ユーザ情報・ソフトカタログファイル５０７を参照することで、そのソフトウェア記憶媒体１を使用したユーザ情報や、そのソフトウェア記憶媒体１に記録されているソフトウェア情報を収集して、その収集・特定結果を集計比較手段５０４に通知する。

【００５３】この収集・特定結果を受け取ると、集計比較手段５０４は、照合分別手段５０３から通知される製造情報に従って、ソフトウェア記憶媒体１に記録された製造時点での使用可能回数をソフトウェア記憶媒体１の識別番号を単位に特定する。そして、復号手段５０２から通知される使用可能回数をソフトウェア記憶媒体１の識別番号を単位に集計し、製造時点での使用可能回数とこの集計値との差分値とからソフトウェアの使用回数を特定して、この特定した使用回数が製造時点での使用可能回数を上回っているか否かをチェックして、そのチェック結果を出力手段５０８に出力する。

【００５４】この構成に従い、本発明では、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。そして、この構成にあって、ソフトウェア記憶媒体１の販売先ユーザ名が特定できるようになっていると、どのユーザが不正複写等の不正使用をしたのかも特定可能となるのである。

【００５５】図示実施例について説明したが、本発明はこれに限定されるものではない。例えば、実施例では、ソフトウェアの使用可能回数の初期値を出荷元で記録していく構成を開示したが、本発明はこれに限られることなく、流通途中の販売店で記録するようにしてもよいのである。また、実施例では、製造時点での使用可能回数がゼロ値に達すると、ユーザサイドでは、使用可能回数の追加を一切認めない構成を開示したが、本発明はこれに限られることなく、使用可能回数の追加を認めていくようにしてもよいのである。また、実施例では、ソフトウェア記憶媒体１を販売する利用形態のもので開示したが、本発明はこれに限られることなく、貸し出す形態のものであってもよいのである。

【００５６】

【発明の効果】以上説明したように、本発明によれば、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されるといったような不正使用にさらされることがあっても、ソ

フトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能回数に従って、その使用可能回数以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになる。しかも、流通途中で暗号構造を変更していくことで、出荷元と中継先との間での不正使用は完全に排除できることになる。

【００５７】そして、本発明によれば、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。しかも、ソフトウェアの流通先を記録しておくことが可能であるならば、誰が不正複写等の不正使用をしたのかも特定可能となる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の適用される流通システムの一例である。

【図３】出荷元装置の装置構成の一実施例である。

【図４】中継先装置の装置構成の一実施例である。

【図５】ソフトウェア読取装置の装置構成の一実施例である。

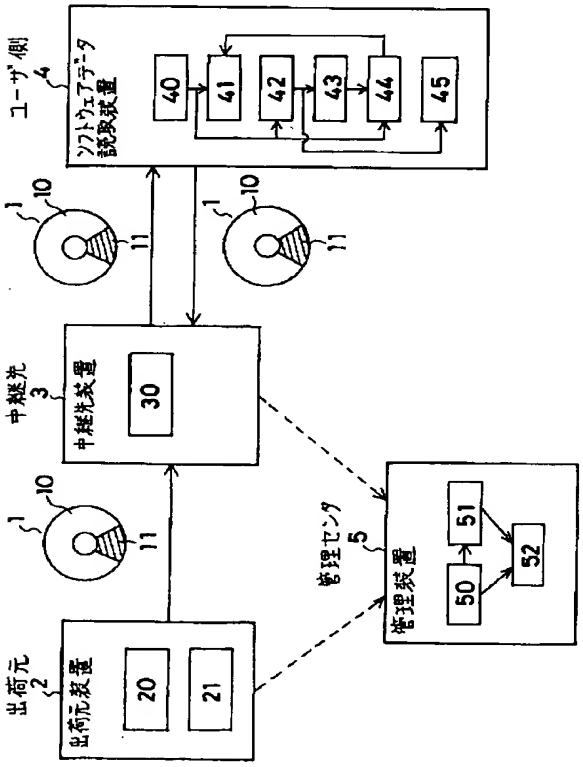
【図６】管理装置の装置構成の一実施例である。

【符号の説明】

１　ソフトウェア記憶媒体
２　出荷元装置
３　中継先装置
４　ソフトウェア読取装置
５　管理装置
１０　書換不可能記憶領域
１１　書換可能記憶領域
２０　第１の書込手段
２１　第２の書込手段
３０　暗号構造変更手段
４０　第１の復号手段
４１　第２の復号手段
４２　算出手段
４３　更新手段
４４　抑止手段
４５　設定手段
５０　第１の集計手段
５１　第２の集計手段
５２　比較手段

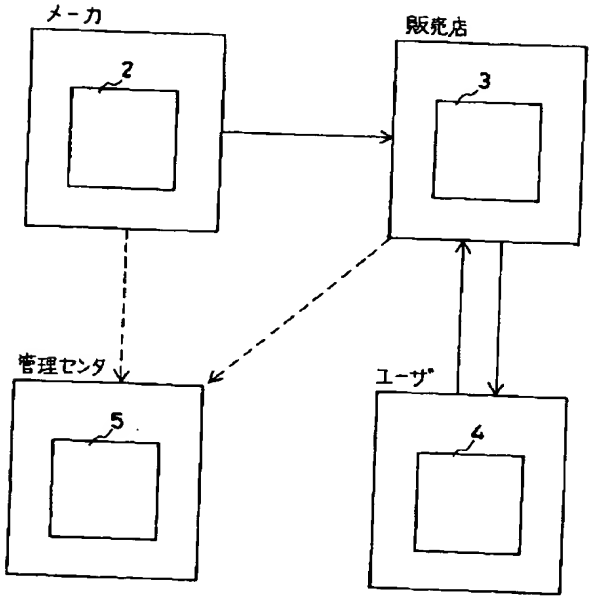
【図１】

本発明の原理構成図



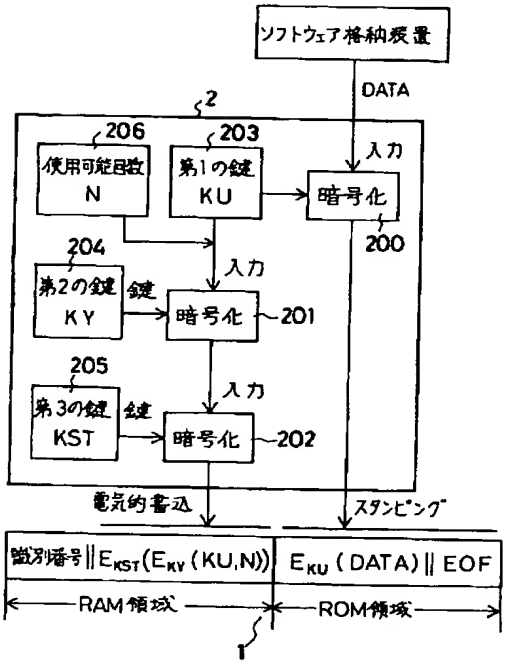
【図２】

本発明の適用される流通システムの一例



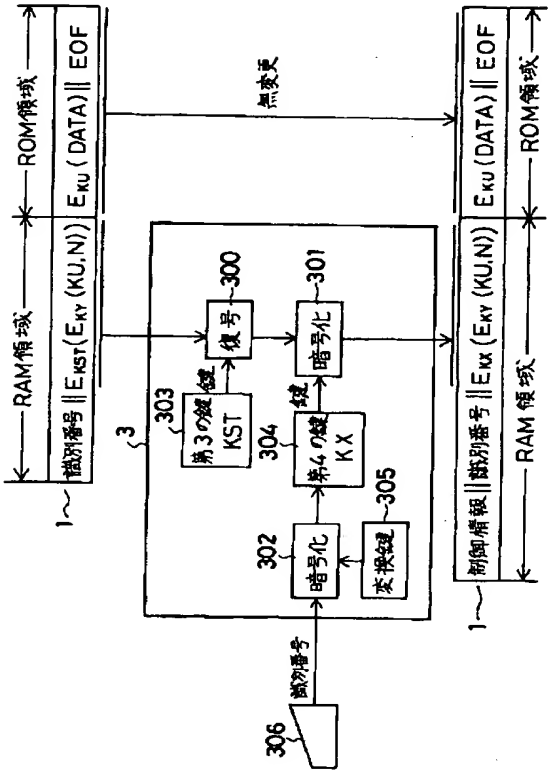
【図3】

出荷元装置の装置構成の一実施例



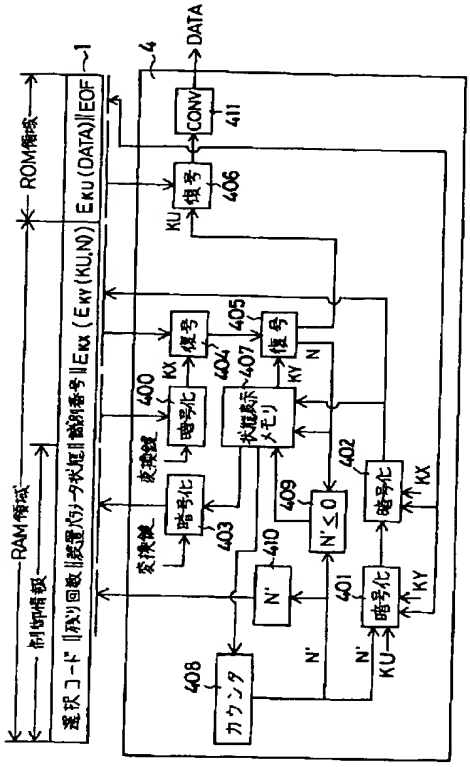
【図4】

中継先装置の装置構成の一実施例



【図５】

ソフトウェア読取装置の装置構成の一実施例



【図６】

管理装置の装置構成の一実施例